

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

WAKABAYASHI, et al
3-14-01
BSKB
(703) 205-8000
1248-0537P
1 of 1

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年 3月14日

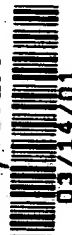
出 願 番 号
Application Number:

特願2000-071183

出 願 人
Applicant(s):

シャープ株式会社
日本電信電話株式会社

11033 U.S. PRO
09/805199

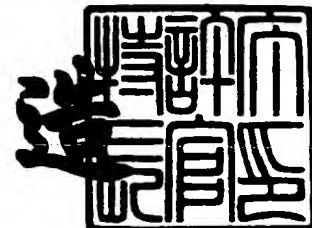


CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 2月 9日

特許庁長官
Commissioner,
Patent Office

及 川 耕 進





【書類名】 特許願

【整理番号】 99J04036

【提出日】 平成12年 3月14日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 G06K 19/00

【発明の名称】 1チップマイクロコンピュータ及びそれを用いたICカード

【請求項の数】 8

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社内

【氏名】 若林 正樹

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社内

【氏名】 小川 竜一

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社内

【氏名】 八重川 和宏

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社内

【氏名】 栗岡 進

【発明者】

【住所又は居所】 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社内

【氏名】 大野 謙次



【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 竹田 忠雄

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 首藤 啓樹

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 吉沢 正浩

【特許出願人】

【識別番号】 000005049

【氏名又は名称】 シャープ株式会社

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100080034

【弁理士】

【氏名又は名称】 原 謙三

【電話番号】 06-6351-4384

【手数料の表示】

【予納台帳番号】 003229

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003082

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 1チップマイクロコンピュータ及びそれを用いたICカード

【特許請求の範囲】

【請求項1】

特定アドレス空間を実行しているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定手段と、

ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、

上記特定アドレス空間を実行しているときに設定可能で、上記アドレス範囲以外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定手段と、

上記判断手段の結果と上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている1チップマイクロコンピュータ。

【請求項2】

特定アドレス空間を実行していることを表すフラグをセットするモニタフラグと、

上記フラグがセットされているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、

ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、

上記フラグがセットされているときに設定可能で、上記アドレス範囲以外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタと、

上記判断手段の結果と上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている1チップマイクロコンピュータ。

【請求項3】

上記特定のアドレス空間には、システムソフトウェアが格納されており、該システムソフトウェアは、次のプログラムを実行する前に、該プログラムの格納されているアドレス範囲を上記アクセス許可アドレス範囲設定レジスタに設定する

と共に、該アドレス範囲外のアドレスに対してアクセスを許可しないように上記アクセス許可レジスタを設定することを特徴とする請求項2に記載の1チップマイクロコンピュータ。

【請求項4】

上記アドレス範囲外のアドレスのアクセスを不許可とする設定がアクセス許可設定レジスタになされており、上記アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断されたとき、割り込み要求信号を生成してCPUへ送る割り込み要求信号生成手段を更に備え、所定の割り込み処理プログラムを実行することを特徴とする請求項2又は3に記載の1チップマイクロコンピュータ。

【請求項5】

上記割り込み処理プログラムは、システムプログラムまたはオペレーティングシステムに制御を移すプログラムであることを特徴とする請求項4に記載の1チップマイクロコンピュータ。

【請求項6】

上記システムソフトウェアが管理する領域に設けられ、メモリへのアクセス制限を越えてアクセスが行われた場合にその旨の情報を記憶する再実行禁止情報記憶手段を更に備え、該情報に基づいて、上記制御手段は上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにすることを特徴とする請求項3に記載の1チップマイクロコンピュータ。

【請求項7】

上記メモリは、書き換え可能な不揮発性メモリであることを特徴とする請求項1、2、3、4、5、又は6に記載の1チップマイクロコンピュータ。

【請求項8】

請求項1、2、3、4、5、6、又は7に記載の1チップマイクロコンピュータを用いたICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、プログラムメモリに複数のアプリケーションプログラムを搭載した1チップマイクロコンピュータ及びそれを用いたICカードに関し、特にメモリへのアクセスを制限し、アプリケーションプログラム間のデータのセキュリティ性を高めた1チップマイクロコンピュータ及びそれを用いたICカードに関するものである。

【0002】

【従来の技術】

大容量不揮発性メモリをプログラムメモリとして搭載した1チップマイクロコンピュータは、各種用途に適した複数のアプリケーションプログラムを予めプログラムメモリに書き込んでおき、それぞれのプログラムを選択し実行処理させることがある。

【0003】

1チップマイクロコンピュータに搭載されている内蔵メモリは、CPUによってアクセスされるため、同一CPUで動作するプログラムは、どのプログラムでもCPUのアクセス可能な範囲のデータに対してアクセスできる。この場合、複数のアプリケーションプログラムを搭載していると、一方のアプリケーションプログラムが他方のアプリケーションプログラムの命令コードやデータにアクセスすることができてしまい、他方のアプリケーションプログラムやデータを改ざんできたり、読み出すことが可能となり、セキュリティ性を損なうという問題を招来していた。

【0004】

上記問題の解決手段として、特開平8-55204号公報には、CPUにプログラムセグメントレジスタとプログラムカウンタとメモリ上のデータをアクセスするためのレジスタとを備え、これらの演算により実行、及び読み書きを行うアドレスを求めてメモリアccessを制限する方法が開示されている。

【0005】

このメモリアccess制限方法を適用したICカードは、図8に示すように、CPU101と、ROM102と、RAM103と、EEPROM104とで構成されており、CPU101の内部構成と機能に上記解決手段が存在している。

【0006】

そして、図9に示すように、このCPU101には、CPU101をリセット後、一度だけ値をリセットすることができるプログラムセグメントレジスタ（PSR）201と、メモリ上のデータをアクセスするためのデータアクセス用オフセットレジスタ（DR）202と、プログラムカウンタ（PC）203及びプログラムセグメントレジスタ201に基づいて実行アドレスを生成するアドレス加算手段205と、データアクセス用オフセットレジスタ202及びプログラムセグメントレジスタ201からデータを読み出して書き込みアドレスを生成するアドレス加算手段204と、実行アドレスの生成とデータ読み出しアドレス及びデータ書き込みアドレスの生成に共通のオフセットアドレス値を生成するアドレス乗算手段206を有している。

【0007】

なお、上記プログラムセグメントレジスタ201は、外部より受け取った目的のアプリケーションプログラムの識別番号を保存しておくために使用される。上記データアクセス用オフセットレジスタ202は、読み書きする際のアドレス値にオフセットを持たせるためのオフセット値を格納するために使用される。

【0008】

また、プログラムカウンタ203は、プログラムの実行命令のアドレスを指し示すものである。例えば、外部より受け取った目的のアプリケーションプログラムの識別番号が2の場合には、その数値2がプログラムセグメントレジスタ201に保存され、絶対オフセット値として実行するアドレスがプログラムセグメントレジスタの1000倍に設定されている場合には、プログラム実行アドレスを（ 2×1000 ）番地へ移行する。以降は、実行アドレスが（ $2 \times 1000 +$ プログラムカウンタ203の値）番地となるように、プログラムセグメントレジスタ201の値とプログラムカウンタ203の値とから実行すべきアドレスを指定する。

【0009】

また、データの読み書きアドレスについては、アドレス（ $2 \times 1000 +$ データアクセス用オフセットレジスタ202の値）番地を特定して実行するように、

プログラムセグメントレジスタ 2 0 1 の値とデータアクセス用オフセットレジスタ 2 0 2 の値から読み書きするアドレスを求める。

【 0 0 1 0 】

上記より、プログラムセグメントレジスタ 2 0 1 に格納された目的のアプリケーションプログラムの識別番号で指定されたアプリケーションプログラムを実行している間は、そのアプリケーションプログラムが格納されたアドレス範囲と R A M 以外に対して、アクセスが不可能となる。

【 0 0 1 1 】

したがって、プログラムメモリに複数のアプリケーションプログラムを搭載する場合に、一方のアプリケーションプログラムが他方のアプリケーションプログラムの命令コードやデータにアクセスすることを不可能とし、これにより、セキュリティ性を確保していた。

【 0 0 1 2 】

【発明が解決しようとする課題】

しかしながら、上記従来のアドレス制限方法では、プログラムセグメントレジスタの設定は一度だけという制約から、C P U のリセット後、一つのアプリケーションプログラムのみ実行可能であり、引き続き他のアプリケーションプログラムを実行するためには、再度、C P U のリセットが必要である。また、アプリケーションプログラム間において通信ができない等、利便性に問題があった。

【 0 0 1 3 】

例えば、複数のアプリケーションプログラムを搭載した I C カードに応用した場合、I C カードを I C カードシステム内のリーダライタから切り離れた状態、つまり、電源を遮断するまで、他のアプリケーションプログラムが実行できない状態となる。

【 0 0 1 4 】

このため、一連の複数のアプリケーションプログラムを実行させようとした場合、一つのアプリケーションプログラムの実行が終了するたびに I C カードをリーダライタから切り離し、再度挿入し、I C カードの初期処理をその度に繰り返す必要が生じ、一連の処理時間が長大化するという問題と、I C カードを何度も

抜き差しする手間が生じるという問題とがあった。

【0015】

また、現在実行中のアプリケーションプログラム内でサブルーチンコール等を行い、元のアドレスに戻したい場合は、一般的にリターンアドレスが一時的にRAMに格納されるが、この値が不具合で又は故意で別の値に書き変わると、アプリケーションプログラムが暴走したり、その他のアプリケーションプログラムをアクセスしてしまう要因となる可能性がある。結果として、CPUは、暴走してしまうことになるが、上記アクセス制限方法では、このような場合の対策が一切講じられていない。

【0016】

そこで、本発明は上記問題点に鑑みなされたものであり、その目的は、複数のアプリケーションプログラムが格納された1チップマイクロコンピュータにおいて、一方のアプリケーションプログラムが他方のアプリケーションプログラムの命令コードやデータにアクセスすることを不可能とし、セキュリティ性を確保した1チップマイクロコンピュータを提供することにある。

【0017】

本発明の他の目的は、複数のアプリケーションプログラムをリセット動作などを必要とせず連続的に実行できるようにして利便性を向上させることが可能な1チップマイクロコンピュータを提供することにある。

【0018】

本発明の更に他の目的は、アプリケーションプログラムがプログラムの不具合または故意に他のアプリケーションプログラムにアクセスすることがあっても、CPUは暴走することなくアクセス制限機能を有効にしたまま処理の継続が行える1チップマイクロコンピュータを提供することにある。

【0019】

【課題を解決するための手段】

本発明に係る1チップマイクロコンピュータは、特定アドレス空間を実行しているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定手段と、ソフトウェアの実行中に、設定された上記アドレス

範囲内でアクセスされているか否かを判断する判断手段と、上記特定アドレス空間を実行しているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定手段と、上記判断手段の結果と上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている。

【 0 0 2 0 】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときに、アクセス許可アドレス範囲設定手段及びアクセス許可設定手段の各設定手段に対して設定可能となる。

【 0 0 2 1 】

上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、たとえ上記特定のアドレス空間から設定しても、アクセス許可アドレス範囲設定手段及びアクセス許可設定手段の各設定手段に対して設定することはできなくなる。

【 0 0 2 2 】

上記特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定手段を介してアドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定手段に入力されていても、該データは該アクセス許可アドレス範囲設定手段に書き込まれることない。

【 0 0 2 3 】

一方、上記特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可設定手段を介して上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定手段に入力されていても、

該データは該アクセス許可設定手段に書き込まれることない。

【 0 0 2 4 】

上記判断手段の判断結果と、上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【 0 0 2 5 】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定手段とアドレス範囲設定手段とに対して設定ができるため、これらの設定手段もアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可手段、アクセス範囲設定手段に対しても影響を与えない。

【 0 0 2 6 】

なお、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されているときには、該アドレス範囲外のアドレスに対してもアクセス可能となる。

【 0 0 2 7 】

本発明に係る他の 1 チップマイクロコンピュータは、特定アドレス空間を実行していることを表すフラグをセットするモニタフラグと、上記フラグがセットされているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、上記フラグがセットされているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタと、上記判断手段の結果と上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するア

クセスを制御する制御手段とを備えている。

【0028】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときにフラグがモニタフラグによってセットされる。フラグがセットされているときに、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対して設定可能となる。

【0029】

フラグがセットされていないときには、特定のアドレス空間に格納されたソフトウェアが実行されていないので、モニタフラグはフラグをセットしない。したがって、このとき、たとえ上記特定のアドレス空間から設定しても、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対する設定はできなくなる。

【0030】

上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタを介してアドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。一方、上記フラグがセットされていないときに、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタに入力されていても、該データは該アクセス許可アドレス範囲設定レジスタに書き込まれることない。

【0031】

これに対して、上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可設定レジスタを介して上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。一方、上記フラグがセットされていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定レジスタに入力されていても、該データは該アクセス許可設定レジスタに書き込まれることない。

【0032】

上記判断手段の判断結果と、上記アクセス許可設定レジスタの設定内容とに基

づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【0033】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定レジスタとアドレス範囲設定レジスタとに対して設定ができるため、これらのレジスタもアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可レジスタ、アクセス範囲設定レジスタにも影響を与えない。

【0034】

なお、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されているときには、該アドレス範囲外のアドレスに対してもアクセス可能となる。

【0035】

上記1チップマイクロコンピュータにおいて、上記特定のアドレス空間には、システムソフトウェアが格納されており、該システムソフトウェアは、次のプログラムを実行する前に、該プログラムの格納されているアドレス範囲を上記アクセス許可アドレス範囲設定レジスタに設定すると共に、該アドレス範囲外のアドレスに対してアクセスを許可しないように上記アクセス許可レジスタを設定することが好ましい。

【0036】

この場合、次のプログラムが実行されるのに先立って、システムソフトウェアは、この実行しようとしている次のプログラムの格納されているアドレス範囲をアクセス許可アドレス範囲設定レジスタに設定する。つまり、実行中のプログラムは、次に実行するプログラムのアドレス範囲が設定されるまで、該次に実行す

るプログラムをアクセスすることはない。

【 0 0 3 7 】

以上のように、オペレーティングシステムなどのシステムソフトウェアからアプリケーションプログラム等の次に実行されるプログラムへ制御が移行される前に、アクセス可能とするアドレス範囲を設定できる。したがって、実行中のプログラムが次に実行されるプログラムに影響を与えることを未然に回避でき、信頼性が著しく向上する。

【 0 0 3 8 】

上記1チップマイクロコンピュータにおいて、上記アドレス範囲外のアドレスのアクセスを不許可とする設定がアクセス許可設定レジスタになされており、上記アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断されたとき、割り込み要求信号を生成してCPUへ送る割り込み要求信号生成手段を更に備え、所定の割り込み処理プログラムを実行することが好ましい。

【 0 0 3 9 】

この場合、他のプログラムによって不正なアクセスがなされたとき、アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断され、割り込み要求信号生成手段によって割り込み要求信号が生成されてCPUへ送られる。CPUは、この割り込み要求信号を受領すると、所定の割り込み処理プログラムが実行されるので、CPUが暴走することを未然に防ぐことができる。

【 0 0 4 0 】

上記1チップマイクロコンピュータにおいて、上記割り込み処理プログラムは、システムプログラムまたはオペレーティングシステムに制御を移すプログラムであることが好ましい。この場合、割り込み要求信号生成手段によって割り込み要求信号が生成されてCPUへ送られると、割り込み処理プログラムが実行され、システムプログラムまたはオペレーティングシステムに制御が移される。これにより、CPUまたはアプリケーションプログラムの暴走を防ぐことが可能となる。

【 0 0 4 1 】

上記1チップマイクロコンピュータにおいて、上記システムソフトウェアが管

理する領域に設けられ、メモリへのアクセス制限を越えてアクセスが行われた場合にその旨の情報を記憶する再実行禁止情報記憶手段を更に備え、該情報に基づいて、上記制御手段は上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないうにすることが好ましい。

【 0 0 4 2 】

この場合、メモリへのアクセス制限を越えてアクセスが行われると、その旨の情報が再実行禁止情報記憶手段（例えば、フラグやレジスタ等）に記憶されることになる。上記制御手段は、この情報に基づいて上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないうにする。これにより、一旦不正なアクセスが行われたプログラムに対しては、それ以降、その実行が禁止されるので、CPUは、暴走することなく処理を継続して行うことが可能となる。

【 0 0 4 3 】

上記1チップマイクロコンピュータにおいて、上記メモリは、書き換え可能な不揮発性メモリであることが好ましい。この場合、後から追加したり、書き換えたりしたプログラム（例えば、アプリケーションプログラム）等が既存のプログラムに影響を与えることなく実行することができる。

【 0 0 4 4 】

上記の1チップマイクロコンピュータは、ICカードに適用することが好ましい。この場合、複数のアプリケーションプログラムを内蔵したICカードにおいて、アプリケーションプログラム間のセキュリティ性を確実に確保することができる。また、複数のプログラムを格納するICカードを実現でき、それぞれのプログラムをリセットすることなく動的に切り換えることができるので、そのICカードをリーダライタに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティ性が確保できるので、個人情報等の機密データを格納するICカードに適している。

【 0 0 4 5 】

【発明の実施の形態】

本発明の実施の一形態について図1乃至図7に基づいて説明すれば、以下のと

おりである。

【 0 0 4 6 】

本実施の形態においては、不揮発性メモリを搭載した I C カード用 1 チップマイクロコンピュータに本発明を適用した場合について説明する。

【 0 0 4 7 】

図 2 は、I C カード用 1 チップマイクロコンピュータのブロック図を示している。この 1 チップマイクロコンピュータは、システムプログラムやアプリケーションプログラムを実行するための C P U 3 0 1 に加えて、システムプログラムやアプリケーションプログラムを格納するための不揮発性メモリ 3 0 3（例えばフラッシュメモリや E E P R O M 等の書き換え可能なメモリ）、C P U 3 0 1 の作業用の R A M 6、メモリ保護回路 5、外部機器と通信を行うための U A R T 2、及びタイマ等周辺回路 4 を備えている。これらのブロックは、C P U 1 が入出力するアドレス線、データ線、データの読み出しや書き込み及びブロック活性化のための制御線などで接続されている。

【 0 0 4 8 】

図 1 は、図 2 のブロック図の C P U 3 0 1、メモリ保護回路 5、不揮発性メモリ 3 0 3 について詳細に説明するブロック図である。

【 0 0 4 9 】

この 1 チップマイクロコンピュータは、C P U 3 0 1 とこれに含まれるプログラムカウンタ（P C）3 0 2 と、不揮発性メモリ 3 0 3 と、モニタフラグ 3 0 4 と、後述するアクセス許可アドレス範囲設定レジスタを含むアクセス許可領域検出回路 3 0 6 と、アクセス許可設定レジスタ 3 0 7 と、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタ 3 0 7 に対する書き込み信号の発生を制限するレジスタ書き込み制御回路 3 0 5 と、不揮発性メモリ 3 0 3 に対して読み出し信号の発生を制限するメモリ読み出し制御回路 3 0 9 と、不揮発性メモリ 3 0 3 に対して書き込み信号の発生を制限するメモリ書き込み制御回路 3 1 0 とを有する。

【 0 0 5 0 】

モニタフラグ 3 0 4 には、C P U 3 0 1 から出力されるアドレスバス信号 3 1

1 と命令の第 1 サイクルを表す命令取り出し信号 3 0 8 (フェッチ) が入力される。ここでは、CPU 3 0 1 が不揮発性メモリ 3 0 3 の特定アドレス空間に格納されたオペレーティングシステムなどのシステムソフトウェアを実行しているか否かの判別が行われる。特定アドレス空間を実行しているとき、モニタフラグ 3 0 4 からは 2 値論理のハイレベル (以下、「1」と称す。) が出力される。一方、特定アドレス空間以外を実行しているとき、モニタフラグ 3 0 4 からは 2 値論理のローレベル (以下、「0」と称す。) が出力される。

【0051】

レジスタ書き込み制御回路 3 0 5 には、CPU 3 0 1 から出力される書き込み基準信号 3 1 2 (ライト) と、モニタフラグ 3 0 4 の出力であるモニタフラグ出力信号 3 1 4 が入力される。書き込み基準信号 3 1 2 は、CPU 3 0 1 が内蔵レジスタや内蔵メモリに書き込みアクセスしたときに出力される信号である。

【0052】

レジスタ書き込み制御回路 3 0 5 では、書き込み基準信号 3 1 2 をアクセス許可領域検出回路 3 0 6 内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ 3 0 7 に伝達するか否かの制御を行う。

【0053】

モニタフラグ 3 0 4 の内容が「1」のとき、つまり、上記特定アドレス空間から書き込み動作が発生したときは、書き込み基準信号 3 1 2 は、後述するレジスタ書き込み信号 3 1 9 として、アクセス許可領域検出回路 3 0 6 内のアクセス許可アドレス範囲設定レジスタ (図示しない) とアクセス許可設定レジスタ 3 0 7 とにそれぞれ伝達される。これにより、アクセス許可領域検出回路 3 0 6 内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ 3 0 7 への書き込みが可能になる。

【0054】

これに対して、モニタフラグ 3 0 4 の内容がデータ「0」のとき、つまり、特定アドレス空間以外から書き込み動作が発生したときは、書き込み基準信号 3 1 2 はアクセス許可領域検出回路 3 0 6 内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ 3 0 7 との何れに対しても伝達されない。これに

より、アクセス許可領域検出回路306内のアクセス許可アドレス範囲設定レジスタとアクセス許可設定レジスタ307への書き込みは禁止される。

【0055】

図3は、図1のブロック図におけるアクセス許可領域検出回路306、アクセス許可設定レジスタ307、メモリ読み出し制御回路309、及びメモリ書き込み制御回路310との動作について、更に詳細に説明したブロック図である。

【0056】

アクセス許可領域検出回路306には、CPU301から出力されるアドレスバス信号311とデータバス信号320と、CPU301から出力される読み出し基準信号313（リード）と、レジスタ書き込み制御回路305の出力であるレジスタ書き込み信号319が入力される。

【0057】

アクセス許可領域検出回路306は、メモリに対して読み出し及び書き込みの制約を解除するアドレス領域を設定するアクセス許可アドレス範囲設定レジスタ401と、アドレス比較回路402とによって構成される。アドレス領域（アクセス許可アドレス範囲）は、例えば、アドレス領域のスタートアドレスとエンドアドレスとを格納するレジスタを用意して設定する。このレジスタは、レジスタ書き込み信号319によって書き込みが行われる。但し、モニタフラグ304によって、上記特定アドレス空間からのみ書き込みが可能である。

【0058】

このアクセス許可領域検出回路306においては、ICカードのアプリケーションプログラムを実行する前に、オペレーティングシステムによってアプリケーションプログラムが格納されているアドレスのスタートアドレスとエンドアドレスが上記アクセス許可アドレス範囲設定レジスタにセットされる。アプリケーションプログラム実行中に、CPU301から出力されるアドレスバス信号311とアクセス許可アドレス範囲設定レジスタ401の値とをアドレス比較回路402で比較することによって設定されたアドレス範囲をCPU301がアクセスしている間は、アドレス比較回路402からアクセス許可アドレス領域出力信号316に、「1」が出力される。また、同様にして、CPU301が、実行中のア

アプリケーションプログラム以外のアプリケーションプログラムが格納されている領域をアクセスした場合、アクセス許可アドレス領域出力信号316に、「0」が出力される。

【0059】

アクセス許可設定レジスタ307には、CPU301から出力されるアドレスバス信号311、データバス信号320、CPU301から出力される読み出し基準信号313、及びレジスタ書き込み制御回路305の出力であるレジスタ書き込み信号319が入力される。

【0060】

このアクセス許可設定レジスタ307は、アクセス許可領域検出回路306内のアクセス許可アドレス範囲設定レジスタ401に設定されたアドレス範囲外のアプリケーションプログラム領域に対して、読み出し又は書き込みのアクセスを許可するか否かを設定するレジスタである。このアクセス許可設定レジスタ307は、レジスタ書き込み信号319によって書き込みが行われる。但し、モニタフラグ304に基づいて、特定アドレス空間からのみ書き込み可能である。

【0061】

ICカードのアプリケーションプログラムを実行する前に、オペレーティングシステムによって、アクセス許可設定レジスタ307に「0」を設定したとき、アクセス許可信号317からは「0」が出力される。また、「1」を設定したとき、アクセス許可信号317からは「1」が出力される。

【0062】

アクセス許可設定レジスタ307は、アクセス許可領域検出回路306内のアクセス許可アドレス範囲設定レジスタ401に設定したアドレス範囲外のアプリケーションプログラム領域に対して、読み出しまたは書き込みのアクセスを許可するか否かを設定するレジスタである。

【0063】

上記のアクセス許可設定レジスタ307の設定内容が「0」のとき、アクセス許可領域検出回路306内のアクセス許可アドレス範囲設定レジスタ401で設定したアプリケーションプログラムアドレス範囲外は、読み出し、及び書き込み

が不可能となる。このアクセス許可設定レジスタ307の内容が「1」のときは、全てのアプリケーションプログラムメモリ領域は読み出し又は書き込みが可能となる。

【0064】

メモリ読み出し制御回路309には、CPU301から出力される読み出し基準信号313、アドレス比較回路402から出力されるアクセス許可アドレス領域出力信号316、及びアクセス許可信号317が入力される。このメモリ読み出し制御回路309は、AND回路403とセクタ回路405により構成される。ここでは、読み出し基準信号313を不揮発性メモリ303に伝達するか否かの制御を行う。

【0065】

アクセス許可信号317から「0」が出力されているとき、セクタ回路405は、読み出し基準信号313とアクセス許可アドレス領域出力信号316をAND回路403に入力して得られる信号を選択して、メモリ303へ読み出し信号318を与える。すなわち、アクセス許可領域検出回路306で設定したメモリ領域以外は、読み出し信号318を出力しない。アクセス許可信号317から「1」が出力されているとき、セクタ回路405は、読み出し基準信号313を選択して、不揮発性メモリ303へ読み出し信号318を与える。すなわち、アプリケーションプログラムメモリ領域であれば、読み出し制限がなくなる。

【0066】

メモリ書き込み制御回路310には、CPU301から出力される書き込み基準信号312、アクセス許可アドレス領域出力信号316、及びアクセス許可信号317が入力される。このメモリ書き込み制御回路310は、AND回路404とセクタ回路406とによって構成される。ここでは、書き込み基準信号312を不揮発性メモリ303に伝達するか否かの制御が行われる。

【0067】

アクセス許可信号317から「0」が出力されているとき、セクタ回路406は、書き込み基準信号312とアクセス許可アドレス領域出力信号316とをAND回路404に入力して得られる信号を選択して、不揮発性メモリ303へ

書き込み信号 315 として出力する。即ち、アクセス許可領域検出回路 306 で設定したメモリ領域外（アドレス範囲外）は、書き込み信号を出力しない。アクセス許可信号 317 から「1」が出力されているとき、セクタ回路 406 は、書き込み基準信号 312 を選択して、不揮発性メモリ 303 へ書き込み信号 315 として出力する。すなわち、アプリケーションプログラムメモリ領域であれば、書き込み制限がなくなる。

【0068】

図 4 は、本実施の形態に係るアプリケーションプログラム格納用の不揮発性メモリ 303 のメモリマップ図である。この不揮発性メモリ 303 には、n 個のアプリケーションプログラム AP1～APn（以下、単に、AP1～APn と称す。）が格納されている。例えば、CPU 301 がオペレーティングシステムにおいて、AP1 のスタートアドレスとエンドアドレスをアクセス許可領域検出回路 306 のアクセス許可アドレス範囲設定レジスタ 401 にセットし、アクセス許可設定レジスタ 307 に「0」をセットして AP1 を実行すると、AP1 以外のアプリケーションプログラムメモリ領域は、アクセス不可となる。

【0069】

図 5 は、CPU 301 が AP1 を実行する前にオペレーティングシステムが行う処理のフローチャートである。まず、ステップ S1、ステップ S2 によって、AP1 のスタートアドレスとエンドアドレスをアクセス許可領域検出回路 306 のアクセス許可アドレス範囲設定レジスタ 401 にセットする。

【0070】

次に、ステップ S3 によって、アクセス許可設定レジスタ 307 に「0」をセットする。次にステップ S4 によって AP1 への分岐命令を実行して、AP1 の実行が開始される。AP1 の実行が終了して、他のアプリケーションプログラムを実行する場合は、そのアプリケーションプログラムに対してステップ S1～S4 の動作を繰り返せばよい。これにより、異なるアプリケーションプログラムを他のアプリケーションプログラムに影響を与えることなく、連続的に実行することが可能となる。

【0071】

また、アプリケーションプログラムメモリに、オペレーティングシステムによってアプリケーションプログラムが新たに追加されたり、入れ替えられた場合にも、そのアプリケーションプログラムのスタートアドレスとエンドアドレスを取得すれば、上記ステップを実行することができる。

【 0 0 7 2 】

図 6 は、1 チップマイクロコンピュータにおいて、図 2 のブロック図の CPU 3 0 1、メモリ保護回路 5、不揮発性メモリ 3 0 3 について、詳細に記載したブロック図である。

【 0 0 7 3 】

この 1 チップマイクロコンピュータは、CPU 3 0 1 とこれに含まれるプログラムカウンタ 3 0 2、不揮発性メモリ 3 0 3、モニタフラグ 3 0 4、アクセス許可設定レジスタ 3 0 7、アクセス許可アドレス範囲設定レジスタ 4 0 1 とアクセス許可設定レジスタ 3 0 7 に対する書き込み信号の発生を制限するレジスタ書き込み制御回路 3 0 5、メモリに対して読み出し信号の発生を制限するメモリ読み出し制御回路 3 0 9、メモリに対して書き込み信号の発生を制限するメモリ書き込み制御回路 3 1 0、及び割り込み制御回路 5 2 1 とを備えている。

【 0 0 7 4 】

図 6 のメモリ読み出し制御回路 3 0 9、メモリ書き込み制御回路 3 1 0、及び割り込み制御回路 5 2 1 以外のブロックの動作は、図 1 のブロック図における動作内容と同一である。

【 0 0 7 5 】

メモリ読み出し制御回路 3 0 9 には、不揮発性メモリ 3 0 3 に対する不許可の読み出し動作が行われたことを示すメモリ読み出し違反検出信号 5 2 2 を出力する機能が追加されている。また、メモリ書き込み制御回路 3 1 0 には、不揮発性メモリ 3 0 3 に対する不許可の書き込み動作が行われたことを示すメモリ書き込み違反検出信号 5 2 3 を出力する機能が追加されている。

【 0 0 7 6 】

割り込み制御回路 5 2 1 は、メモリ読み出し制御回路 3 0 9 より出力されるメモリ読み出し違反検出信号 5 2 2 と、メモリ書き込み制御回路 3 1 0 から出力さ

れるメモリ書き込み違反検出信号523とを入力とし、CPU301に対して割り込み要求信号524を出力する。

【0077】

メモリ読み出し制御回路309に、「0」のアクセス許可信号317が入力されているとき、すなわち不揮発性メモリ303に対して読み出し及び書き込みの不許可が設定されているときに、アクセス許可アドレス領域検出回路306で許可したアドレス範囲外に対してCPU301が読み出し動作を行った場合、メモリ読み出し違反検出信号522が活性化される（アクティブになる）。

【0078】

メモリ書き込み制御回路310に、「0」のアクセス許可信号317が入力されているとき、すなわち不揮発性メモリ303に対して読み出し及び書き込みの不許可が設定されているときに、アクセス許可アドレス領域検出回路306で許可したアドレス領域外に対してCPU301が書き込み動作を行った場合、メモリ書き込み違反検出信号523が活性化される。

【0079】

それぞれのメモリアクセス違反検出信号は、割り込み制御回路521に入力されており、この回路からCPU301に対して割り込み要求信号524として伝達される。したがって、CPU301は、実行中のアプリケーションプログラムが、それ以外のプログラムメモリの領域に対して不正アクセスしたときに、割り込み処理を行うことが可能になる。

【0080】

不揮発性メモリ303への読み出しと書き込みとは同時に行われないので、割り込み制御回路521は、メモリ読み出し違反検出信号522及びメモリ書き込み違反検出信号523を入力とするOR回路と、CPU301の仕様に合わせてタイミングを制御する公知のタイミング制御回路（図示しない）とで構成でき、その出力で割り込み要求信号524を生成する。

【0081】

図7は、上記メモリアクセス違反を検出して割り込み要求信号524が発生した場合のCPU301とオペレーティングシステムが管理する割り込み処理の一

例をフローチャートで表したものである。

【 0 0 8 2 】

CPU301に割り込み要求信号524が入力されると、割り込み処理プログラムが起動される。まず、ステップS11において、アクセス違反を起こしたアプリケーションプログラム（AP）の使用した作業領域などの初期化を行う。次に、ステップS12においてアクセス違反を起こしたアプリケーションプログラム（AP）が再度実行されないように、オペレーティングシステムが管理する領域に用意された実行禁止を制御するフラグ又はレジスタをセットし、該アプリケーションプログラムが再度実行されることが禁止される。次に、ステップS13においてオペレーティングシステムへのリターンアドレス（復帰アドレス）をセットし、割り込み処理を終了して、オペレーティングシステムへ制御が移る。

【 0 0 8 3 】

これにより、アプリケーションプログラムのアクセス違反が発生しても、CPU301が暴走することなく処理を継続することが可能となる。上記ステップS12においてフラグ又はレジスタが一旦セットされると、それ以降は、該アプリケーションプログラムが再度実行されることはない。つまり、フラグ又はレジスタがセットされていることが確認されると、該当するアプリケーションプログラムが再度実行されることはない。

【 0 0 8 4 】

図示はしないが、以上に詳述した1チップマイクロコンピュータをICカードに搭載することによって、不揮発性メモリ303に複数のプログラムを格納でき、それぞれのプログラムを上述の従来技術のようにシステムをリセットすることなく動的に切り換えることができるので、そのICカードをリーダーライターに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティが確保できるため、個人情報等の機密データを格納するICカードに適している。

【 0 0 8 5 】

上述の説明では、説明の便宜上、各種レジスタや各種フラグを例に挙げて説明

したが、本発明はこれに限定されるものではなく、同様の機能を有する記憶手段で代用してもよい。

【 0 0 8 6 】

本発明に係る 1 チップマイクロコンピュータは、以上のように、内蔵メモリとしてプログラム用メモリ及び作業用メモリを含むものであって、プログラムの実行命令のアドレスを指し示すプログラムカウンタを含む CPU と、特定アドレス空間を実行していることを表すモニタフラグと、特定のアドレス空間からのみ設定が可能で、メモリに対して読み出しや書き込みのアクセス許可を設定するレジスタと、アクセスを許可するアドレス範囲を設定するレジスタと、内蔵メモリに対する読み出し信号、書き込み信号を制御する制御回路とを備えている。

【 0 0 8 7 】

上記発明によれば、アプリケーションプログラム格納用メモリのうち、実行中のアプリケーションプログラムが格納されている領域以外は、アクセス不可となり、他のアプリケーションプログラムが格納された領域に悪影響を及ぼすことがない。つまり、実行中のアプリケーションプログラムは、他のアプリケーションプログラムが格納された領域に悪影響を及ぼさない。また、オペレーティングシステムなどのシステムプログラム（システムソフトウェア）が格納された特定領域からのみ、アクセス許可レジスタとアドレス範囲設定レジスタへ設定できるため、これらのレジスタもアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可レジスタ、アクセス範囲設定レジスタにも影響を与えない。

【 0 0 8 8 】

上記 1 チップマイクロコンピュータにおいて、特定領域からアクセス許可アドレス範囲設定レジスタやアクセス許可レジスタへデータを設定する手段を更に備えていることが好ましい。この場合、オペレーティングシステムからアプリケーションプログラムへ制御を移行する前に、アクセス可能とするアドレス範囲を設定でき、実行中のアプリケーションプログラムが他のアプリケーションプログラムへ影響を与えることがなくなる。

【 0 0 8 9 】

上記 1 チップマイクロコンピュータにおいて、実行中のアプリケーションプログラムが格納されているメモリ以外をアクセスしたとき、CPUへ割り込み要求信号を発生する手段を更に設けていることが好ましい。この場合、アプリケーションプログラムによって不正なアクセスがなされたとき、これを割り込み要求信号としてCPUが検出できるため、CPUまたはアプリケーションプログラムの暴走を未然に防ぐことが可能となる。

【 0 0 9 0 】

上記 1 チップマイクロコンピュータにおいて、実行中のアプリケーションプログラムが格納されているメモリ以外をアクセスしたときに、CPUまたはアプリケーションプログラムの暴走を防ぐCPUの割り込み処理プログラムを内蔵する構成が好ましい。この場合、アプリケーションプログラムによって不正なアクセスがなされたとき、割り込み処理プログラムを実行する（例えば、システムプログラムまたはオペレーティングシステムに制御を移す）ことによって、CPUまたはアプリケーションプログラムの暴走を防ぐことが可能となる。

【 0 0 9 1 】

上記 1 チップマイクロコンピュータにおいて、プログラムメモリがフラッシュメモリやEEPROMなどの書き換え可能な不揮発性メモリであることが好ましい。この場合、アプリケーションプログラムを後から追加したり、書き換えたりしても、既存のアプリケーションプログラムに影響を与えることなく、プログラムを実行することができる。

【 0 0 9 2 】

上記 1 チップマイクロコンピュータにおいて、内蔵メモリ内へのアクセス制限を越えてアクセスが行われた場合に、アクセスを行ったプログラムの実行の禁止を制御する、システムプログラムまたはオペレーティングシステムが管理する領域に用意されたフラグまたはレジスタを有することが好ましい。この場合、アプリケーションプログラムを後から追加したり、書き換えたりしても、既存のアプリケーションプログラムに影響を与えることなく、プログラムを実行することが可能となる。一旦不正なアクセスを行ったプログラムは、以降、その実行が禁止されるため、CPUが暴走することなく処理を継続することが可能となる。

【 0 0 9 3 】

上記 1 チップマイクロコンピュータにおいて、プログラムメモリがフラッシュメモリや E E P R O M などの書き換え可能な不揮発性メモリで構成することが好ましい。この場合、後から追加したり、書き換えたアプリケーションプログラムが、既存のアプリケーションプログラムに影響を与えることなく、プログラムを実行できる。

【 0 0 9 4 】

上記 1 チップマイクロコンピュータは I C カード用に好適である。この場合、複数のアプリケーションプログラムを内蔵した I C カードにおいて、アプリケーションプログラム間のセキュリティ性を確保することができる。また、複数のプログラムを格納する I C カードを実現でき、それぞれのプログラムをリセットすることなく動的に切り換えることができるので、その I C カードをリーダライタに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティが確保できるので、個人情報等の機密データを格納する I C カードに適している。

【 0 0 9 5 】

【発明の効果】

本発明に係る 1 チップマイクロコンピュータは、特定アドレス空間を実行しているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定手段と、ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、上記特定アドレス空間を実行しているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定手段と、上記判断手段の結果と上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている。

【 0 0 9 6 】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定手

段を介してアドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定手段に入力されていても、該データは該アクセス許可アドレス範囲設定手段に書き込まれることない。

【 0 0 9 7 】

一方、上記特定のアドレス空間に格納されたソフトウェアが実行されているときに、上記特定のアドレス空間からアクセス許可設定手段を介して上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。一方、上記特定のアドレス空間に格納されたソフトウェアが実行されていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定手段に入力されていても、該データは該アクセス許可設定手段に書き込まれることない。

【 0 0 9 8 】

上記判断手段の判断結果と、上記アクセス許可設定手段の設定内容とに基づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【 0 0 9 9 】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定手段とアドレス範囲設定手段とに対して設定ができるため、これらの設定手段もアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可手段、アクセス範囲設定手段に対しても影響を与えないという効果を奏する。

【 0 1 0 0 】

本発明に係る他の1チップマイクロコンピュータは、特定アドレス空間を実行していることを表すフラグをセットするモニタフラグと、上記フラグがセットされているときに設定可能で、アクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、ソフトウェアの実行中に、設定された上記アドレス範囲内でアクセスされているか否かを判断する判断手段と、上記フラグがセットされているときに設定可能で、上記アドレス範囲外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタと、上記判断手段の結果と上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するアクセスを制御する制御手段とを備えている。

【0101】

上記の発明によれば、特定のアドレス空間に格納されたソフトウェアが実行されているときにフラグがモニタフラグによってセットされる。フラグがセットされているときに、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対して設定可能となる。

【0102】

フラグがセットされていないときには、特定のアドレス空間に格納されたソフトウェアが実行されていないので、モニタフラグはフラグをセットしない。したがって、このとき、たとえ上記特定のアドレス空間から設定しても、アクセス許可アドレス範囲設定レジスタ及びアクセス許可設定レジスタの各レジスタに対する設定はできなくなる。

【0103】

上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタを介して、アドレス範囲が設定できる。この場合、ソフトウェアの実行中に、該設定されたアドレス範囲内のアドレスに対してアクセスされているか否かが判断手段によって判断される。これに対して、上記フラグがセットされていないときに、いくらデータが上記特定のアドレス空間からアクセス許可アドレス範囲設定レジスタに入力されていても、該データは該アクセス許可アドレス範囲設定レジスタに書き込まれることない。

【0104】

一方、上記フラグがセットされているときに、上記特定のアドレス空間からアクセス許可設定レジスタを介して、上記アドレス範囲外のアドレスのアクセスを許可するか否かが設定できる。これに対して、上記フラグがセットされていないときには、いくらデータが上記特定のアドレス空間からアクセス許可設定レジスタに入力されていても、該データは該アクセス許可設定レジスタに書き込まれることない。

【0105】

上記判断手段の判断結果と、上記アクセス許可設定レジスタの設定内容とに基づいて、メモリに対するアクセスが制御手段によって制御される。すなわち、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されていないときには、メモリにおいて、該アドレス範囲内のアドレスに対してのみアクセス可能となる一方、該アドレス範囲外のアドレスに対してはアクセスはできない。

【0106】

このようにメモリに対するアクセスを制御することによって、実行中のプログラムが他のプログラムが格納されているアドレス空間に悪影響を及ぼすことを未然に回避できる。また、特定のアドレス空間からのみ、アクセス許可設定レジスタとアドレス範囲設定レジスタとに対して設定ができるため、これらのレジスタもアプリケーションプログラムから影響を受けない。つまり、特定アドレス空間からのみアクセス可能なアクセス許可レジスタ、アクセス範囲設定レジスタにも影響を与えない。また、アドレス範囲が設定されていて、且つ、アドレス範囲外のアドレスのアクセスが許可されているときには、該アドレス範囲外のアドレスに対してもアクセス可能となるという効果を併せて奏する。

【0107】

上記1チップマイクロコンピュータにおいて、上記特定のアドレス空間には、システムソフトウェアが格納されており、該システムソフトウェアは、次のプログラムを実行する前に、該プログラムの格納されているアドレス範囲を上記アクセス許可アドレス範囲設定レジスタに設定すると共に、該アドレス範囲外のアドレスに対してアクセスを許可しないように上記アクセス許可レジスタを設定する

ことが好ましい。

【0108】

この場合、次のプログラムが実行されるのに先立って、システムソフトウェアは、この実行しようとしている次のプログラムの格納されているアドレス範囲をアクセス許可アドレス範囲設定レジスタに設定する。つまり、実行中のプログラムは、次に実行するプログラムのアドレス範囲が設定されるまで、該次に実行するプログラムをアクセスすることはない。

【0109】

これにより、オペレーティングシステムなどのシステムソフトウェアからアプリケーションプログラム等の次に実行されるプログラムへ制御が移行される前に、アクセス可能とするアドレス範囲を設定できる。したがって、実行中のプログラムが次に実行されるプログラムに影響を与えることを未然に回避でき、信頼性が著しく向上するという効果を奏する。

【0110】

上記1チップマイクロコンピュータにおいて、上記アドレス範囲外のアドレスのアクセスを不許可とする設定がアクセス許可設定レジスタになされており、上記アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断されたとき、割り込み要求信号を生成してCPUへ送る割り込み要求信号生成手段を更に備え、所定の割り込み処理プログラムを実行することが好ましい。

【0111】

この場合、他のプログラムによって不正なアクセスがなされたとき、アドレス範囲外のアドレスに対してアクセスしたことが判断手段によって判断され、割り込み要求信号生成手段によって割り込み要求信号が生成されてCPUへ送られる。CPUは、この割り込み要求信号を受領すると、所定の割り込み処理プログラムが実行されるので、CPUが暴走することを未然に防ぐことができるという効果を奏する。

【0112】

上記1チップマイクロコンピュータにおいて、上記割り込み処理プログラムは、システムプログラムまたはオペレーティングシステムに制御を移すプログラム

であることが好ましい。

【 0 1 1 3 】

この場合、割り込み要求信号生成手段によって割り込み要求信号が生成されて CPU へ送られると、割り込み処理プログラムが実行され、システムプログラムまたはオペレーティングシステムに制御が移される。これにより、CPU またはアプリケーションプログラムの暴走を防ぐことが可能となるという効果を奏する。

【 0 1 1 4 】

上記 1 チップマイクロコンピュータにおいて、上記システムソフトウェアが管理する領域に設けられ、メモリへのアクセス制限を越えてアクセスが行われた場合にその旨の情報を記憶する再実行禁止情報記憶手段を更に備え、該情報に基づいて、上記制御手段は上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにすることが好ましい。

【 0 1 1 5 】

この場合、メモリへのアクセス制限を越えてアクセスが行われると、その旨の情報が再実行禁止情報記憶手段（例えば、フラグやレジスタ等）に記憶されることになる。上記制御手段は、この情報に基づいて上記メモリを制御し、アクセス制限を越えて上記アクセスが再度行われないようにする。これにより、一旦不正なアクセスが行われたプログラムに対しては、それ以降、その実行が禁止されるので、CPU は、暴走することなく処理を継続して行うことが可能となるという効果を奏する。

【 0 1 1 6 】

上記 1 チップマイクロコンピュータにおいて、上記メモリは、書き換え可能な不揮発性メモリであることが好ましい。

【 0 1 1 7 】

この場合、後から追加したり、書き換えたりしたプログラム（例えば、アプリケーションプログラム）等が既存のプログラムに影響を与えることなく実行することができるという効果を奏する。

【 0 1 1 8 】

上記の 1 チップマイクロコンピュータは、I C カードに適用することが好ましい。

【0 1 1 9】

この場合、複数のアプリケーションプログラムを内蔵した I C カードにおいて、アプリケーションプログラム間のセキュリティ性を確実に確保することができる。また、複数のプログラムを格納する I C カードを実現でき、それぞれのプログラムをリセットすることなく動的に切り換えることができるので、その I C カードをリーダライタに挿入した状態で多目的に利用できる。さらに、複数のプログラム及びデータ間の干渉を禁止できるため、不正なプログラムのアクセス防止やデータの保護等のセキュリティ性が確保できるので、個人情報等の機密データを格納する I C カードに適しているという効果を併せて奏する。

【図面の簡単な説明】

【図 1】

本発明の 1 チップマイクロコンピュータの構成例を示すブロック図である。

【図 2】

上記 1 チップマイクロコンピュータの具体例を示すブロック図である。

【図 3】

アクセス許可領域検出回路とアクセス制御回路周辺の構成例を示すブロック図である。

【図 4】

本発明に係る 1 チップマイクロコンピュータのアプリケーションプログラム用メモリのメモリマップ図である。

【図 5】

上記アプリケーションプログラムの分岐時のフローチャートである。

【図 6】

本発明の 1 チップマイクロコンピュータの構成例を示すブロック図である。

【図 7】

メモリ不正アクセス時の割り込み処理フローチャートである。

【図 8】

従来の1チップマイクロコンピュータの構成例を示すブロック図である。

【図9】

従来のCPUの構成機能図である。

【符号の説明】

- 3 0 1 CPU
- 3 0 2 プログラムカウンタ
- 3 0 3 不揮発性メモリ
- 3 0 4 モニタフラグ
- 3 0 5 レジスタ書き込み制御回路
- 3 0 6 アクセス許可領域検出回路
- 3 0 7 アクセス許可設定レジスタ
- 3 0 8 命令取り出し信号
- 3 0 9 メモリ読み出し制御回路
- 3 1 0 メモリ書き込み制御回路
- 3 1 1 アドレスバス信号
- 3 1 2 書き込み基準信号
- 3 1 3 読み出し基準信号
- 3 1 4 モニタフラグ出力信号
- 3 1 5 メモリ書き込み信号
- 3 1 6 アクセス許可アドレス範囲設定レジスタ出力信号
- 3 1 7 アクセス許可設定レジスタ出力信号
- 3 1 8 メモリ読み出し信号
- 3 1 9 レジスタ書き込み信号
- 3 2 0 データバス信号
- 4 0 1 アクセス許可アドレス範囲設定レジスタ
- 4 0 2 アドレス比較回路
- 4 0 3 AND回路
- 4 0 5 セレクタ回路
- 5 2 1 割り込み制御回路

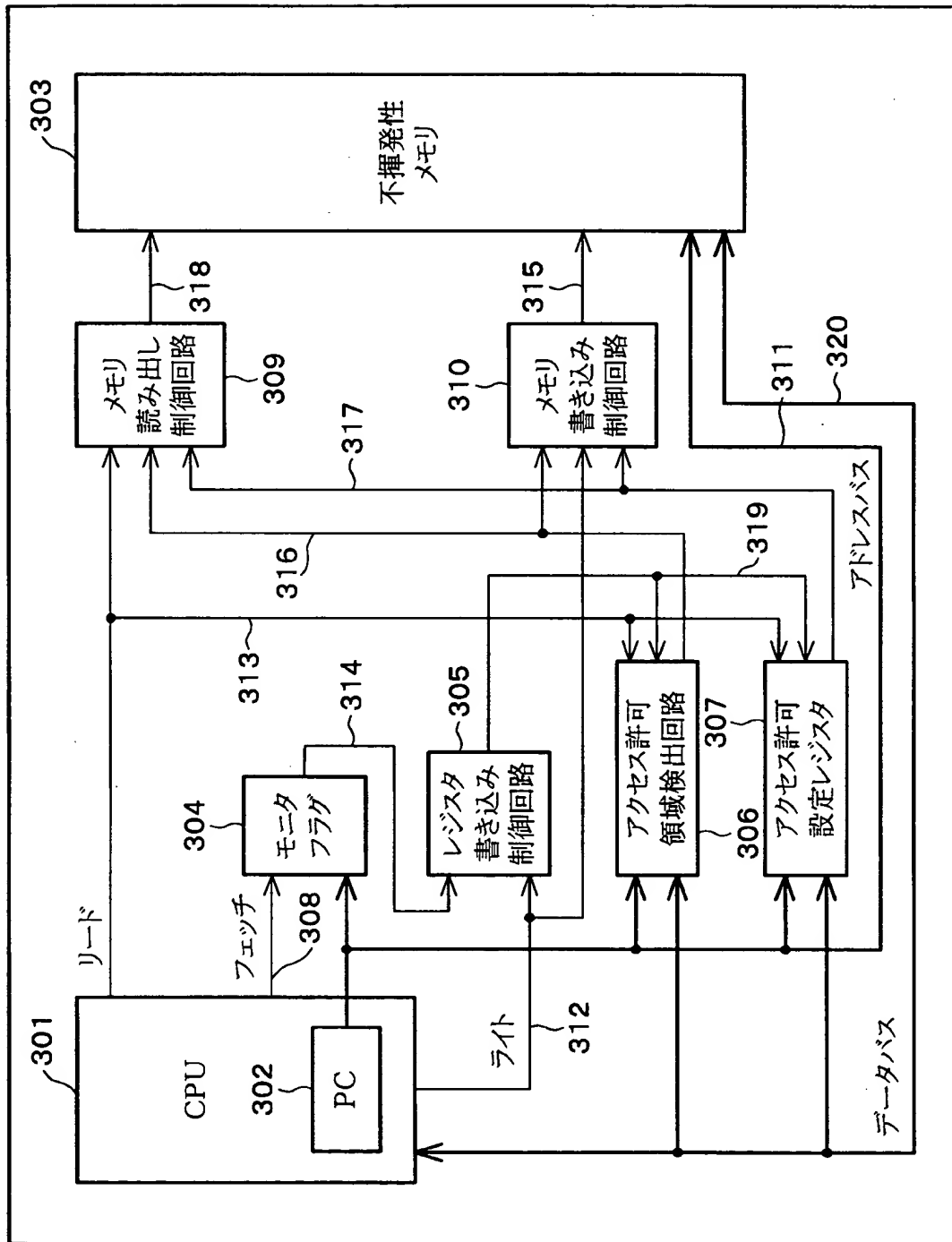
5 2 2 メモリ読み出し違反検出信号

5 2 3 メモリ書き込み違反検出信号

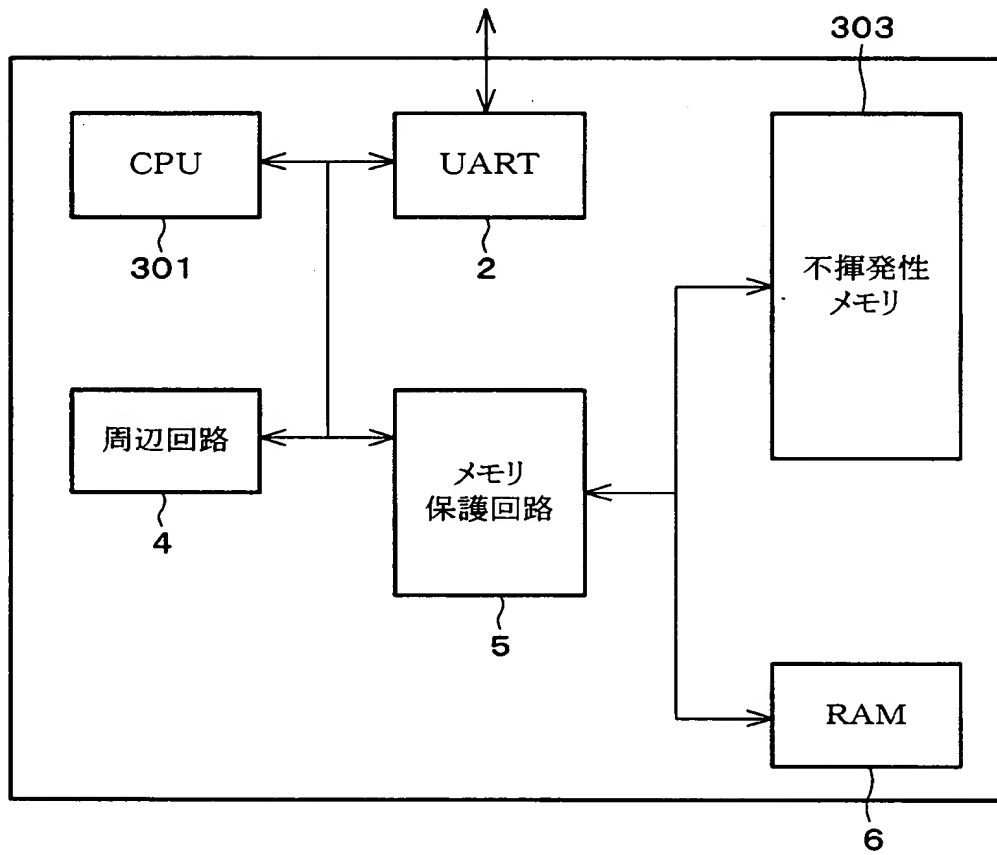
5 2 4 割り込み要求信号

【書類名】 図面

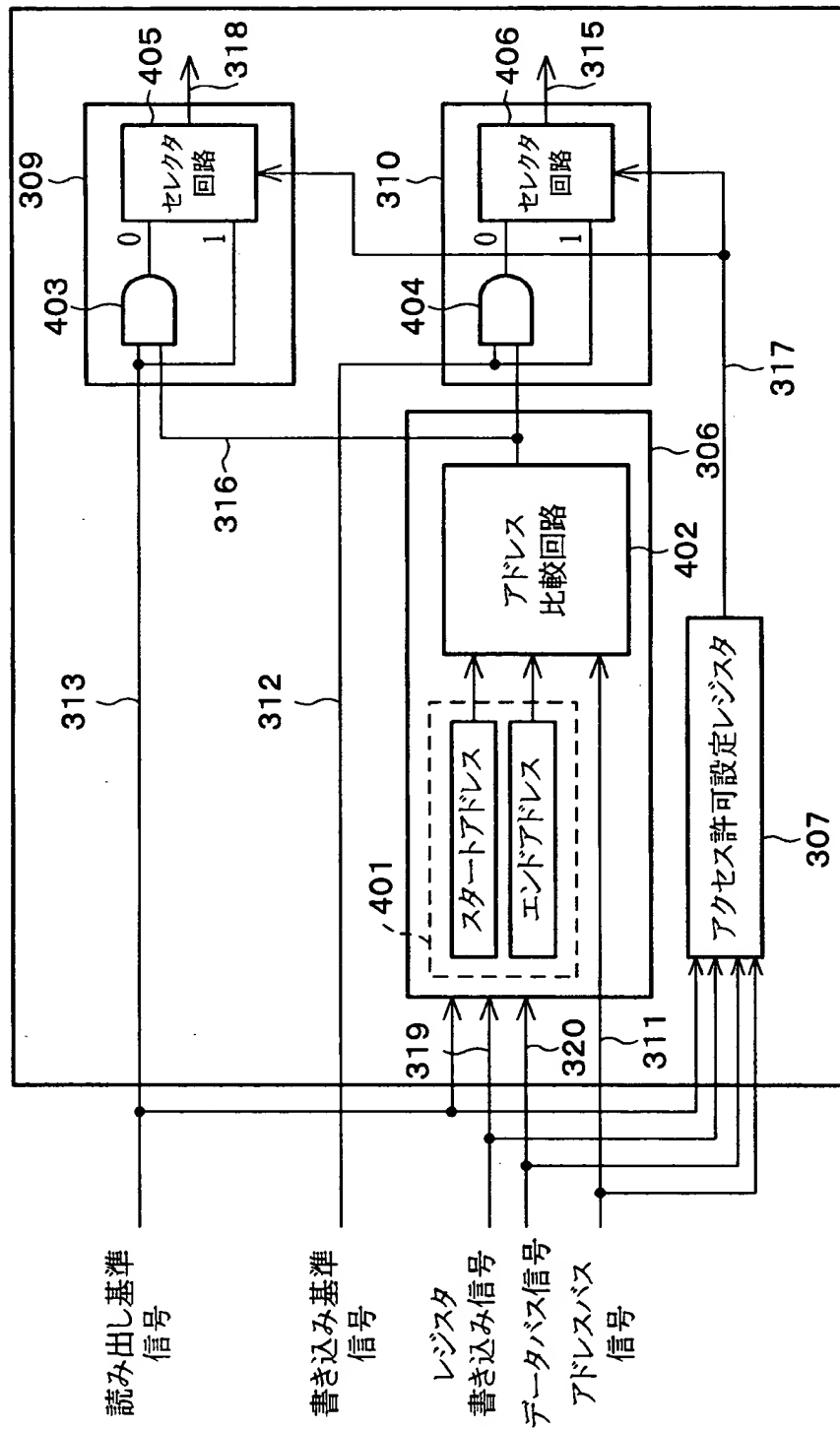
【図 1】



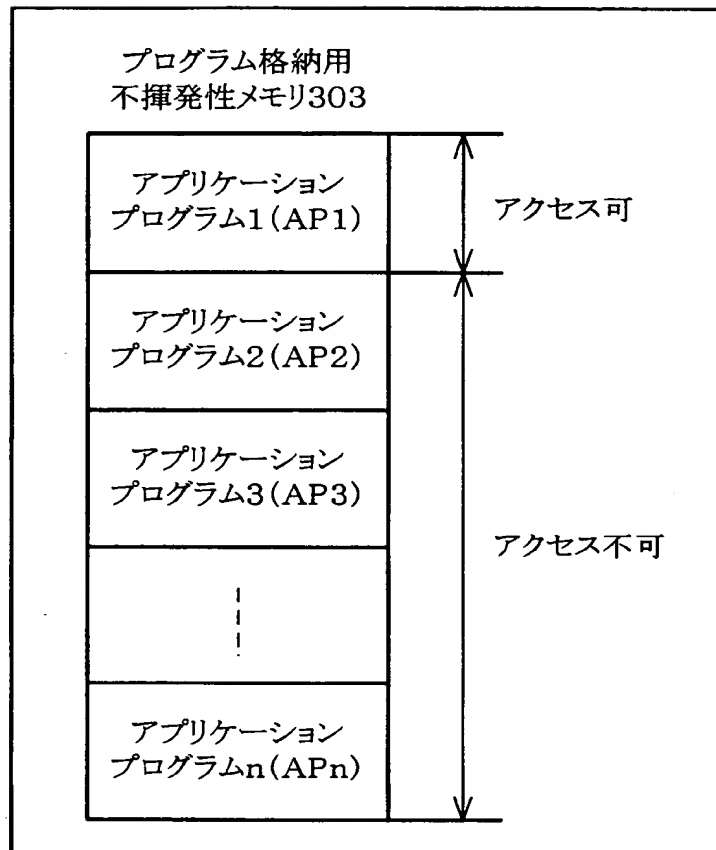
【図 2】



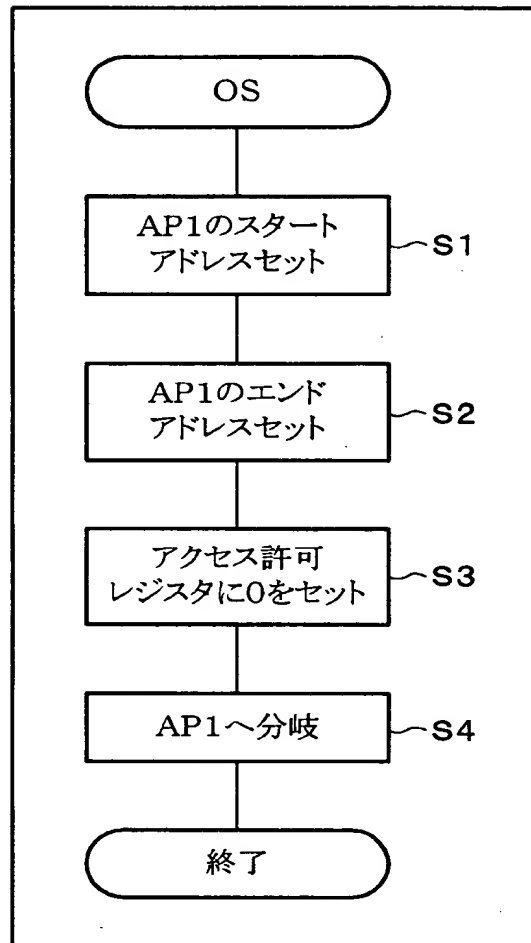
【図 3】



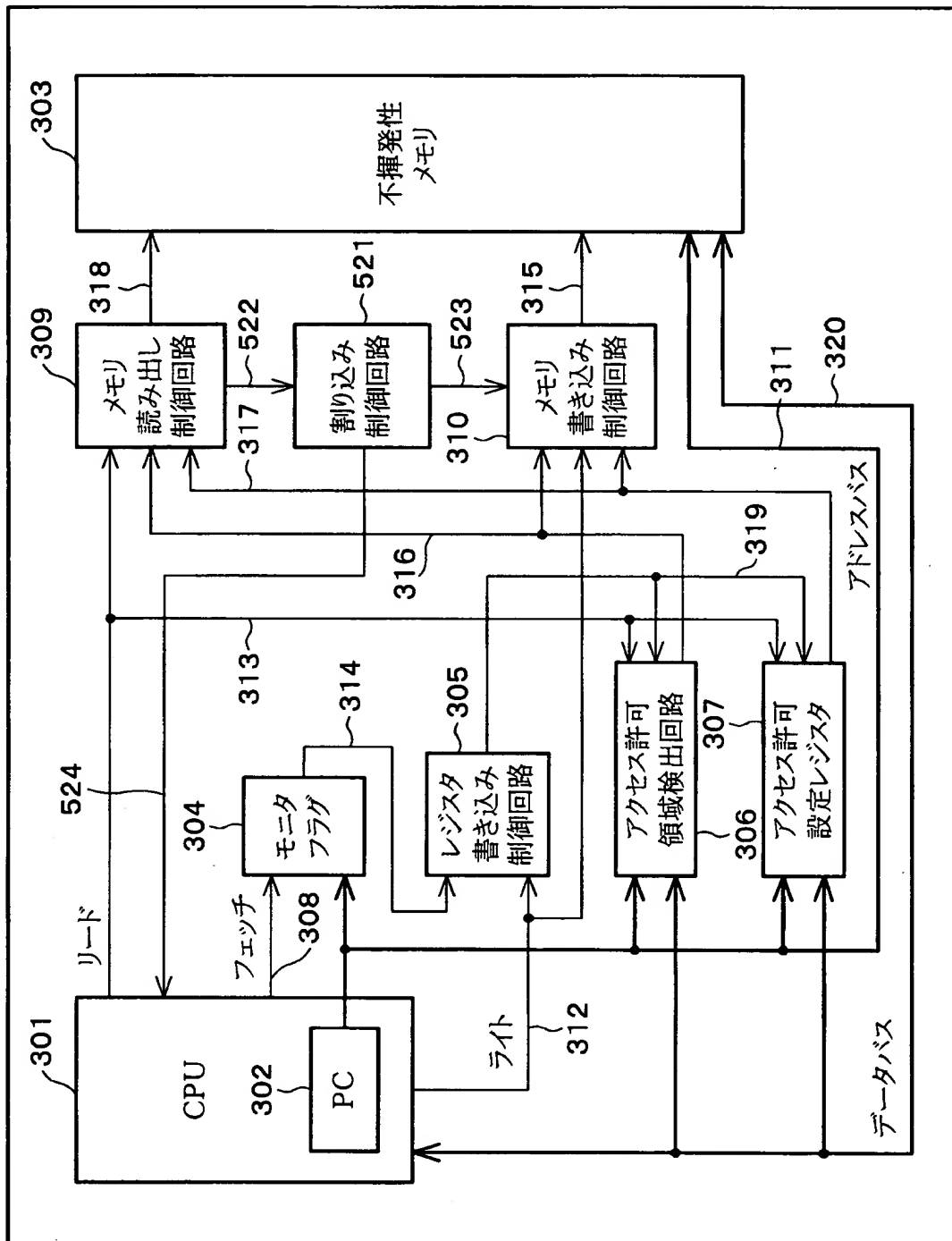
【図 4】



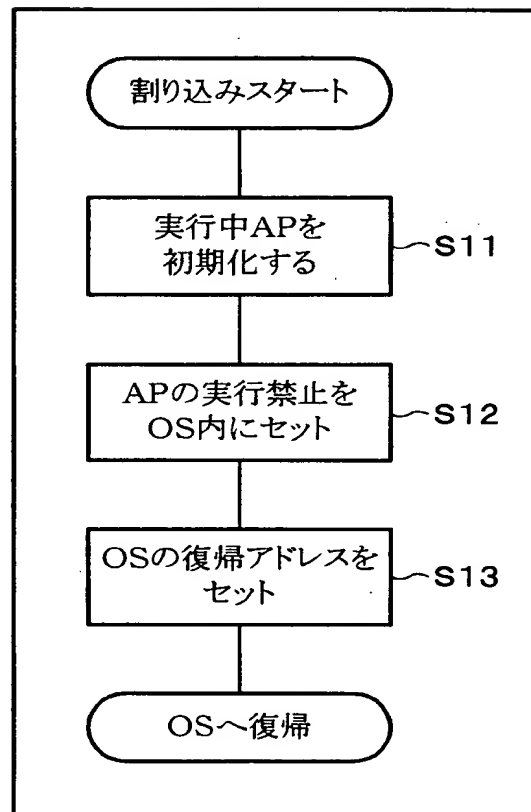
【図5】



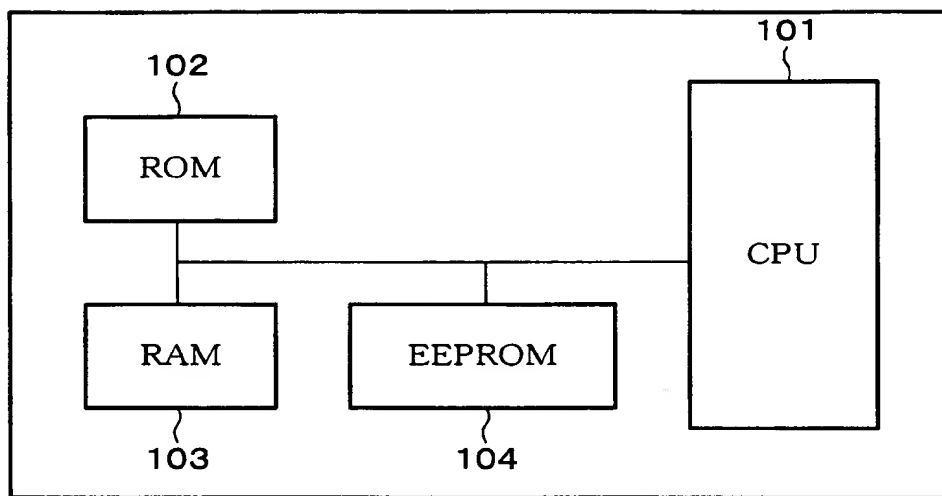
【図 6】



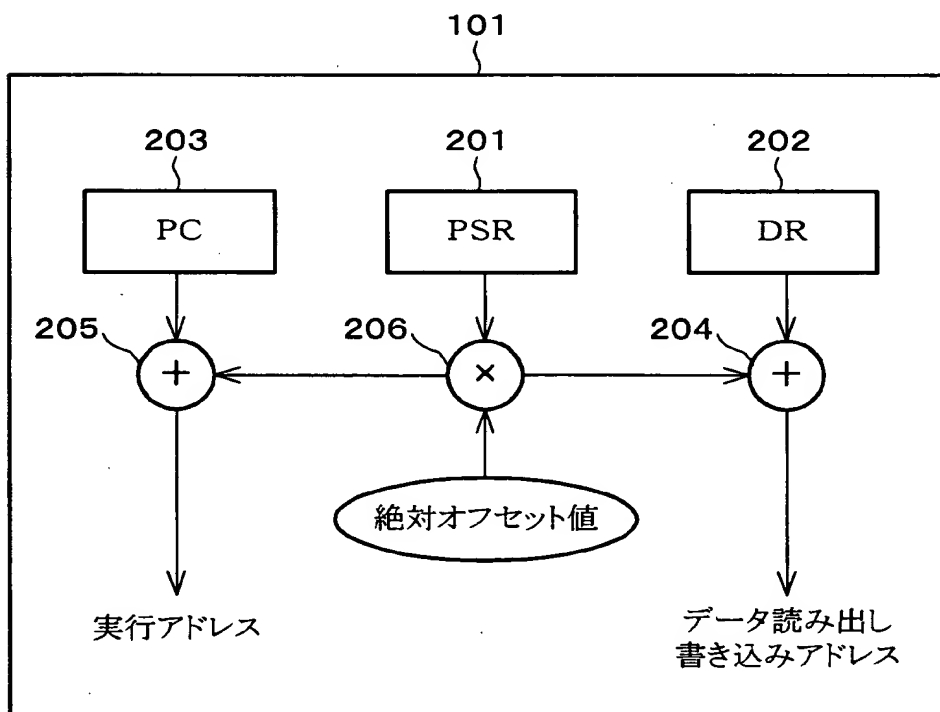
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 アプリケーションプログラム間のセキュリティ性を確保した 1 チップマイクロコンピュータを提供する。

【解決手段】 本発明の 1 チップマイクロコンピュータは、特定アドレス空間を実行していることを表すフラグをセットするモニタフラグ 3 0 4 と、上記フラグがセットされているときにアクセスを許可するアドレス範囲を設定するアクセス許可アドレス範囲設定レジスタと、設定された上記アドレス範囲内でアクセスされているか否かを判断するアクセス許可領域検出回路 3 0 6 と、上記アドレス範囲以外のアドレスのアクセスを許可するか否かを設定するアクセス許可設定レジスタ 3 1 9 と、上記判断結果と上記アクセス許可設定レジスタ 3 1 9 の設定内容とに基づいて、不揮発性メモリ 3 0 3 に対するアクセスを制御するメモリ読み出し制御回路 3 0 9 及びメモリ書き込み回路 3 1 0 とを備えている。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005049]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	大阪府大阪市阿倍野区長池町22番22号
氏 名	シャープ株式会社

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社